International Journal of All Research Education and Scientific Methods (IJARESM),
ISSN: 2455-6211, Volume 13, Issue 5, May-2025, Available online at: www.ijaresm.com

Enhancing Security in Wearable Computing: A Lightweight Authenticated Key Exchange Scheme

Sunkara Venkata Dharani Teja Sree[1] , Uma Maheswara Rao Mogili[2], Krishna Veni Ampoly[3]

[1]Avanthi's St Theressa Institute of Engineering and Technology , Department of Computer Science and Engineering, Garividi, Andhra Pradesh, India
[2,3]Assistant Professor, Avanthi's St Theressa Institute of Engineering and Technology , Department of Computer Science and Engineering, Garividi, Andhra Pradesh, India

---

ABSTRACT

Wearable computing presents vast potential to enhance quality of life, but it also introduces significant privacy and security challenges. Existing authentication and key exchange schemes often involve high computational and communication overhead, making them unsuitable for resource-constrained wearable devices. To address these challenges, we propose EAKE-WC—an Efficient and Anonymous Authenticated Key Exchange scheme for Wearable Computing. EAKE-WC supports mutual authentication between users, wearable devices, and cloud servers, and establishes session-specific secret keys for secure communication. It utilizes lightweight cryptographic primitives, including ASCON (Authenticated Encryption with Associated Data), bitwise XOR, and hash functions, to ensure strong security with minimal resource consumption. To enhance trust and manage user credentials securely, the scheme integrates a credential revocation mechanism that enables the timely and secure removal of compromised or expired credentials without impacting system performance. Security analysis and performance evaluation confirm that EAKE-WC meets the stringent requirements of wearable computing, outperforming existing schemes in terms of efficiency, security, revocation handling, and overall functionality.

Index Terms—Key Exchange, Authentication, Authenticated Encryption With Associated Data, Wearable Computing, Security.

INTRODUCTION

Wearable devices are dedicated communication devices that are usually embedded in clothing pieces or any other wear- able accessory or worn directly on the body. Through its connection to the Internet and integration with different software applications, users can sense and track their physiological and ambient environmental conditions. They can directly view, react to, and send information without a manual process. Its applications span across different industries, such as mobile payment, social networking, casual games, audio-visual entertainment, positioning and navigation, and health management [1]. Currently, wearable devices primarily consist of smart watches and bracelets, smart shoes, smart clothing, smart glasses (primarily VR/AR headsets), smart accessories, and ear-mounted devices. In medical applications, wearable devices are utilized for monitoring multiple physiological parameters of patients, such as multiple blood-based readings (glucose level, blood pressure, and blood oxygen level), heart rate, and body temperature [2]. Typically, the data collected is initially transmitted from a wearable device to the user's mobile terminal via a wireless protocol for further processing and then transferred by the mobile device to the cloud for analysis. In addition, the physician keeps track of the patient's health status remotely through connectivity to the cloud server and provides treatment suggestions.

With the development of hardware and software technology, smart wearable devices will appear everywhere in our daily life and bring us much convenience. But the installed programs and wearable devices in the wear- able computing environment have security and privacy concerns. Moreover, the application of wireless transmission technology in the wear- able computing environment, where data collecting, storage, and transmission are more vulnerable to multiple attacks, is a more serious security issue [3], [4].

An authenticated key exchange (AKE) scheme is a common security solution that provides security protection against multiple possible security attacks, e.g., "de-synchronization", "ephemeral secret leakage (ESL)", "replay", "impersonation", etc. AKE allows two authentic parties to authenticate mutually and set up a secure communication channel. After being successfully authenticated, both parties obtain a common session key to encrypt and decrypt data exchanged over the open

channel to facilitate future secure communication. AKE schemes are a good means of promoting secure and private communication between two parties [5]. Several cryptographic primitives have been utilized in the different authentication schemes applied in the environment of wire-less communications [6], [7]. These schemes employ different cryptographic primitives, e.g., public key cryptography schemes [8], [9], hybrid schemes on the cryptographic hash function and symmetric technology [10], [11], and cryptographic hash function-based schemes [12], [13]. Since wearable devices are constrained in resources, most wearable computing environments employ authentication schemes that make use of lightweight cryptographic primitives, such as symmetric cryptography and cryptographic hash functions [14]. Though most possible security attacks can be countered to a degree by the existing AKE schemes in wire-less environments, a number of them have been found to fail their claimed security requirements. To ensure secure communication within wearable computing settings, we come up with a more robust, reliable, and ultralightweight AKE scheme.

RELATED WORK

New researchers have designed various AKE schemes for resource-constrained devices in wearable computing scenarios. The goal is to achieve maximum performance with minimized overheads based on the premise that mutual authentication and key agreement are achieved as securely as they could be. In [16], Wang et al. briefly mentioned the performance metric of anonymous two-factor authentication schemes in light of the overwhelming list of security needs (e.g., resistance to impersonation attacks) and desirable features (e.g., user anonymity). They then present a counterargument to Huang et al.'s [17] unsolved challenge.

A light-weight anonymous user AKE scheme, put forward by Gupta et al. [18], was designed using bitwise XOR operations as well as hash functions, and mutual authentication between the device and user mobile terminal is achieved through the aid of the cloud server. Nevertheless, Hajian et al. [19] analyzed Gupta et al.'s scheme and showed how it can be compromised using the privileged insider, de-synchronization, and offline password guessing attacks.

Alternatively, Liu et al. [20] introduced an asymmetric three-party-based AKE scheme utilizing the visual out-of-band channel and quick response code to achieve mutual authentication between wearable devices and mobile terminals. Likewise, for improved security in healthcare systems, Wu et al. [21] designed an anonymous two-factor AKE scheme. Nevertheless, their suggested scheme is susceptible to privileged insider and de-synchronization attacks.

Yet another new bio-hashing-based AKE scheme was proposed by Li et al. [22]. Their suggested scheme, however, cannot provide user anonymity and is susceptible to privileged insider and sensor node capture attacks. Ali et al. [24] researched the security weaknesses existing in Amin et al.'s work [23] and proposed an enhanced three-factor-based secure remote user authentication scheme.

Das et al. [25] had suggested a wearable device mutual authentication scheme. Nevertheless, Das et al.'s scheme is vulnerable to de-synchronization attacks [26]. Srinivas et al. [27] suggested a cloud-based authentication scheme using hash functions and Chinese Remainder Theorem in 2020, which achieve mutual authentication between re- mote users and wearable sensor nodes and can resist potential security attacks.

In [28], Guo et al. designed an anonymous and effi- cient AKE scheme for wearable computing. The proposed scheme reduced the computation overhead by employing bit- wise XOR operations and a large number of hash functions. Fotouhi et al. [29] designed a lightweight two-factor-based AKE scheme for the Internet of medical things. However, Li et al. [30] pointed out that Fotouhi et al. [29] cannot resist sensor physical capture and stolen verifier attacks.

Wazid et al. [31] designed and performed testbed experi- ments of the user AKE scheme for smart healthcare. However, the proposed scheme cannot resist de-synchronization attacks. In [32], Wang et al. proposed a physical unclonable function (PUF) and blockchain-based AKE scheme for wireless medical sensor networks. However, Yu and Park [33] indicated that Wang et al.’s scheme [32] does not provide mutual authentication and is not secured against session key disclosure and MitM attacks. To address the limitations of Wang et al.’s scheme [32], Yu and Park [33] devised an improved version of their scheme.

Proposed Scheme

This section presents the proposed EAKE-WC scheme for wearable computing environments to ensure that only authorized users can access the deployed wearable devices.The proposed EAKE-WC is based on the preloaded key method and utilizes the secure hash algorithm (SHA-256) with ASCON AEAD primitive. Furthermore, it is assumed that the time of

every entity in the wearable computing environment is synchronized. The EAKE-WC is divided into five phases, each of which is described in further detail below:

1. **System Initialization Phase:**
   In this phase, the trusted authority (TA) or administrator sets up the system parameters required for secure communication.

- Each wearable device and user device is preloaded with a unique identifier (ID) and a shared secret key.
- Cryptographic primitives such as SHA-256 (for hashing) and ASCON AEAD (for authenticated encryption) are selected.
- Public parameters for secure operation are published, while secret values remain protected.
- All devices synchronize their clocks to ensure that timestamps in the communication process remain consistent.

2. Registration Phase:
Before any communication happens, users and wearable devices must register with the system.

- The user submits their identity information securely to the trusted authority.
- The trusted authority verifies the user and generates credentials for them, binding their identity to a pre-shared secret key.
- Similarly, wearable devices are registered and linked to their respective secret keys and identifiers.
- After registration, both users and devices are equipped with the necessary cryptographic materials for authentication.

3. Authentication and Key Exchange Phase:
This is the main phase where secure mutual authentication and session key establishment occur.

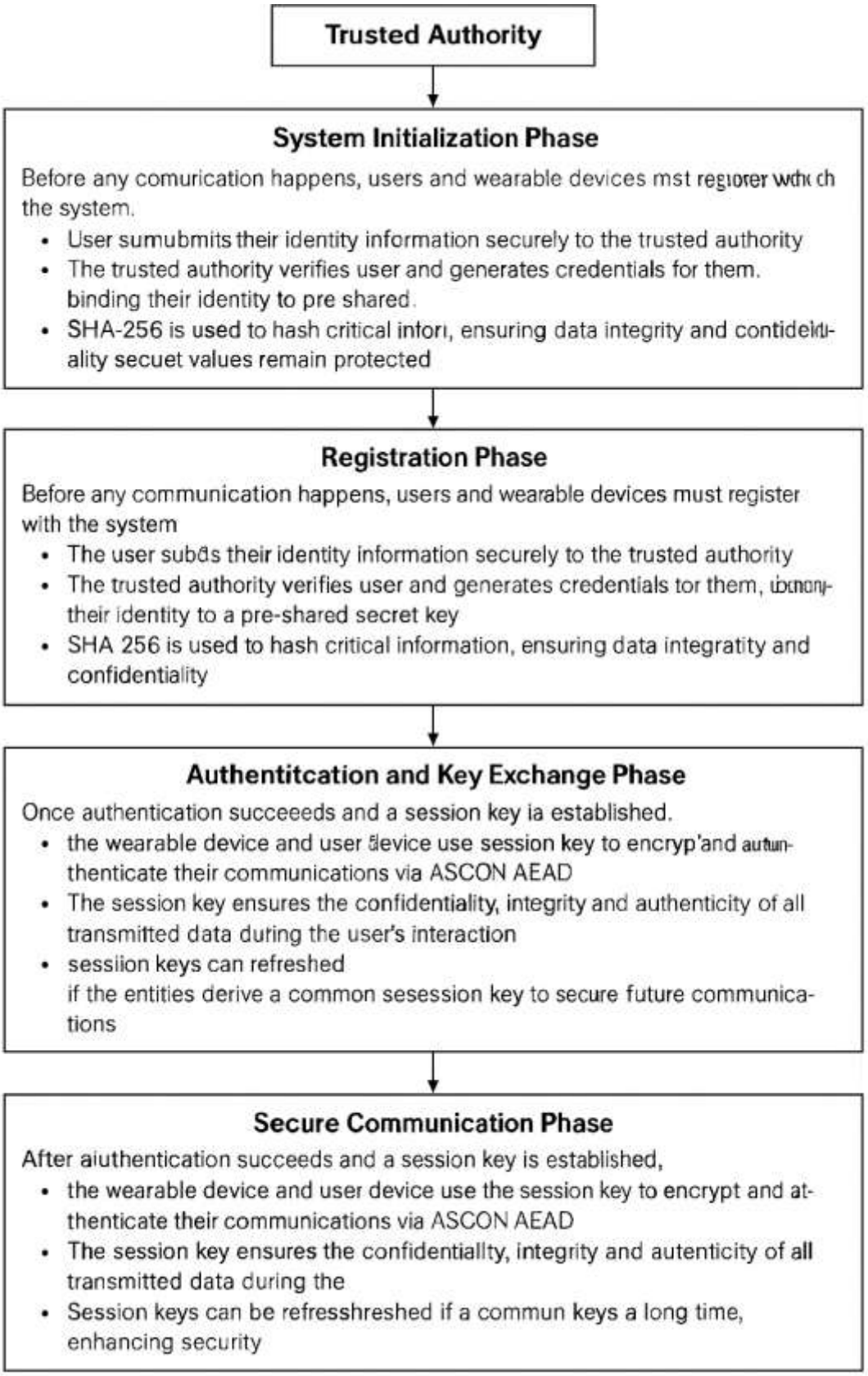
- When a user attempts to access a wearable device, the device and user perform a mutual challenge-response protocol.
- Nonces (random numbers) and timestamps are exchanged to guarantee freshness and prevent replay attacks.
- SHA-256 is used to hash critical information, ensuring data integrity and confidentiality.
- ASCON AEAD is applied to encrypt and authenticate the exchanged messages, protecting them against tampering.
- If all verifications succeed, both entities derive a common session key to secure future communications.

4. Secure Communication Phase:
Once authentication succeeds and a session key is established:

- The wearable device and user device use the session key to encrypt and authenticate their communications via ASCON AEAD.
- The session key ensures the confidentiality, integrity, and authenticity of all transmitted data during the user's interaction with the wearable device.
- Periodically, session keys can be refreshed if the communication lasts a long time, enhancing security.

5. Session Termination Phase:
After the secure communication session is complete:

- Both the user device and the wearable device securely erase the session key to prevent any potential leakage.
- Optionally, a logout or session end acknowledgment is exchanged between the user and the device.
- Any subsequent communication would require a new authentication and key exchange process to maintain security.


Trusted Authority
System Initialization Phase
Before any comurication happens, users and wearable devices mst regiorer wdh ch the system.
• User sumubmits their identity information securely to the trusted authority
• The trusted authority verifies user and generates credentials for them. binding their identity to pre shared.
• SHA-256 is used to hash critical infori, ensuring data integrity and contidelu-ality secuet values remain protected
Registration Phase
Before any communication happens, users and wearable devices must register with the system
• The user subds their identity information securely to the trusted authority
• The trusted authority verifies user and generates credentials tor them, ubmony-their identity to a pre-shared secret key
• SHA 256 is used to hash critical information, ensuring data integratity and confidentiality
Authentitcation and Key Exchange Phase
Once authentication succeeeds and a session key ia established.
• the wearable device and user device use session key to encryp'and autun-thenticate their communications via ASCON AEAD
• The session key ensures the confidentiality, integrity and authenticity of all transmitted data during the user's interaction
• sessiion keys can refreshed
if the entities derive a common sesession key to secure future communica-tions
Secure Communication Phase
After aiuthentication succeeds and a session key is established,
• the wearable device and user device use the session key to encrypt and at-thenticate their communications via ASCON AEAD
• The session key ensures the confidentiallty, integrity and autenticity of all transmitted data during the
• Session keys can be refresshreshed if a commun keys a long time, enhancing security

CONCLUSION

The present study introduced EAKE-WC, an effective and anonymous authenticated key exchange scheme suitable for wearable computing. By utilizing lightweight cryptography primitives like XOR, ASCON, and the hash function, we established two secret session keys, ensuring secure communication between the wearable device, the user, and the cloud server. The security analysis demonstrated that EAKE- WC complied with the security requirements of wearable computing. Additionally, the comparative analysis showed thatour proposed scheme surpassed state-of-the-art benchmark schemes regarding communication and computational over- head. As a result, EAKE-WC delivered improved security and performance in the wearable computing environment.

Despite offering security against common attacks in wear- able computing, we acknowledge the potential for physical tampering attacks on the wearable device. Therefore, we pro- pose future work to incorporate Physical Unclonable Functions (PUFs) into the design of EAKE-WC to address this limitation. Additionally, we intend to evaluate EAKE-WC in a real-world setting to refine the scheme further, if required, to provide enhanced security and better performance.

REFERENCES

[1]. S. Seneviratne *et al.*, "A survey of wearable devices and challenges,"*IEEE Commun. Surv. Tutor.*, vol. 19, no. 4, pp. 2573-2620, Jul. 2017.
[2]. A. Pantelopoulos and N. G. Bourbakis, "A survey on wearable sensor- based systems for health monitoring and prognosis," *IEEE Trans. Syst. Man Cybern. Part C (Applications and Reviews)*, vol. 40, no. 1, pp. 1-12, Jan. 2010.
[3]. O. Arias, J. Wurm, K. Hoang and Y. Jin, "Privacy and security in Internet of things and wearable devices," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 1, no. 2, pp. 99-109, April-June 2015.
[4]. J. Zhou, Z. Cao, X. Dong, and X. Lin, "Security and privacy in cloud- assisted wireless wearable communications: Challenges, solutions, and future directions," *IEEE Wirel. Commun.*, vol. 22, no. 2, pp. 136-144, Apr. 2015.
[5]. Y. K. Ever, "Secure-anonymous user authentication scheme for e- Healthcare application using wireless medical sensor networks," *IEEE Syst. J.*, vol. 13, no. 1, pp. 456-467, Mar. 2019.
[6]. A. Badshah, M. Waqas, F. Muhammad, G. Abbas, Z. H. Abbas, S. A. Chaudhry and S. Chen. "AAKE-BIVT: Anonymous Authenticated Key Exchange Scheme for Blockchain-Enabled Internet of Vehicles in Smart Transportation," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 1739-1755, Feb. 2023.
[7]. A. Badshah, M. Waqas, F. Muhammad, G. Abbas and Z. H. Abbas, "A Novel Framework for Smart Systems Using Blockchain-Enabled Internet of Things," in *IT Professional*, vol. 24, no. 3, pp. 73-80, May 2022.
[8]. D. He, S. Zeadally, N. Kumar, and J. H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Syst. J.*, vol. 11, no. 4, pp. 2590-2601, 2017.
[9]. J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *J. Netw. Comput. Appl.*, vol. 106, pp. 117- 123, Mar. 2018.
[10]. J. Liu and K. S. Kwak, "Hybrid security mechanisms for wireless body area networks," *ICUFN 2010 - 2nd International Conference on Ubiquitous and Future Networks*, (Jeju, South Korea), 16-18 June 2010,pp. 98-103.
[11]. Q. Xie, D. S. Wong, G. Wang, X. Tan, K. Chen, and L. Fang, "Provably secure dynamic ID-based anonymous two-factor authenticated key exchange protocol with extended security model," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 6, pp. 1382-1392, Jan. 2017.
[12]. L. Zhang, Y. Zhang, S. Tang, and H. Luo, "Privacy protection for e- health systems by means of dynamic authentication and three-factor key agreement," *IEEE Trans. Ind. Electron.*, vol. 65, no. 3, pp. 2795-2805, Mar. 2018.
[13]. M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 2,pp. 391-406, 1 Mar.-Apr. 2020.
[14]. B. Gong, G. Zheng, M. Waqas, S. Tu and S. Chen, "LCDMA: Lightweight Cross-domain Mutual Identity Authentication Scheme for Internet of Things," in *IEEE Internet of Things Journal*, Mar. 2023.
[15]. S. Botsa and M. N. Bhat, "Blockchain based Authentication Techniques for Internet of Medical Things," 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS), Hassan, India, 2024, pp. 1-4, doi: 10.1109/IACIS61494.2024.10721657.
[16]. D. Wang, D. He, P. Wang, and C. -H. Chu, "Anonymous Two-Factor Authentication in Distributed Systems: Certain goals are beyond attain- ment," IEEE Trans. Dependable Secure Comput., vol. 12, no. 4, pp. 428- 442, July-Aug. 2015.

[17]. X. Huang, X. Chen, J. Li, Y. Xiang, and L. Xu, "Further observations on smart-card-based password-authenticated key agreement in distributed systems," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 7, pp. 1767- 1775, Jul. 2014.
[18]. A. Gupta, M. Tripathi, T. J. Shaikh, and A. Sharma, "A lightweight anonymous user authentication and key establishment scheme for wear- able devices," Comput. Netw., vol. 149, pp. 29-42, Feb. 2019.
[19]. R. Hajian, S. ZakeriKia, S. H. Erfani, and M. Mirabi, "SHAPARAK: Scalable healthcare authentication protocol with attack-resilience and anonymous key-agreement," Comput. Netw., vol. 183, article no. 107567, Dec. 2020.
[20]. S. Liu, S. Hu, J. Weng, S. Zhu, and Z. Chen, "A novel asymmetric three- party based authentication scheme in wearable devices environment," J. Netw. Comput. Appl., vol. 60, pp. 144-154, Jan. 2016.
[21]. F. Wu, L. Xu, S. Kumari, and X. Li, "An improved and anonymous two- factor authentication protocol for healthcare applications with wireless medical sensor networks," Multimedia Syst., vol. 23, no. 2, pp. 195-205, Mar. 2017.
[22]. X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, and M. K. Khan, "A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity," Secur. Commun. Netw., vol. 9, no. 15, pp. 2643-2655, Oct. 2016.
[23]. R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, and N. Kumar, "A robust and anonymous patient monitoring system using wireless medical sensor networks," Future Gener. Comput. Syst., vol. 80, pp. 483-495, Mar. 2018.
[24]. R. Ali, A. K. Pal, S. Kumari, A. K. Sangaiah, X. Li, and F. Wu, "An enhanced three-factor based authentication protocol using wireless medical sensor networks for healthcare monitoring," J. Ambient Intell. Humanized Comput., vol. 269, pp. 1-22, Sep. 2018.
[25]. A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K. K. R. Choo, andY. H. Park, "Design of secure and lightweight authentication protocol for wearable devices environment," IEEE J. Biomed. Health Inform., vol. 22, no. 4, pp. 1310-1322, Jul. 2018.
[26]. Q. Jiang, Y. Qian, J. Ma, X. Ma, Q. Cheng, and F. Wei, "User centric three-factor authentication protocol for cloud-assisted wearable devices," Int. J. Commun. Syst., vol. 32, no. 6, pp. 1-20, Apr. 2019.
[27]. J. Srinivas, A. K. Das, N. Kumar, and J. Rodrigues, "Cloud centric authentication for wearable healthcare monitoring system," IEEE Trans. Dependable Secure Comput., vol. 17, no. 5, pp. 942-956, Sep./Oct. 2020.
[28]. Y. Guo, Z. Zhang, and Y. Guo, "Anonymous authenticated key agreement and group proof protocol for wearable computing," IEEE Trans. Mobile Comput., vol. 21, no. 8, pp. 2718-2731, Aug. 2022.
[29]. M. Fotouhi, M. Bayat, A. K. Das, H. A. N. Far, S. M. Pournaghi, and M.A. Doostari, "A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT," Comput. Netw., vol. 177, pp. 1-16, Aug. 2020.
[30]. J. Li, Z. Su, D. Guo, K.-K. R. Choo, and Y. Ji, "PSL-MAAKA: Provably secure and lightweight mutual authentication and key agreement protocol for fully public channels in Internet of Medical Things," IEEE Internet Things J., vol. 8, no. 17, pp. 13183-13195, Sep. 2021.
[31]. M. Wazid, S. Thapliyal, D. P. Singh, A. K. Das, and S. Shetty, "Design and testbed experiments of user authentication and key establishment mechanism for smart healthcare cyber-physical systems," IEEE Trans. Netw. Sci. Eng., early access, Mar. 2022.
[32]. W. Wang et al., "Blockchain and PUF-based lightweight authentication protocol for wireless medical sensor networks," IEEE Internet Things J., vol. 9, no. 11, pp. 8883-8891, June 2022.